LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

UCRL-CONF-226691

Use of Commercial I&C in the Next Generation of Nuclear Power

G. L. Johnson

June 6, 2006

Technology Roadmap on Instrumentation, Control, and Human Machine Interface to Support DOE Advanced Nuclear Power Plant Programs
Reno, NV, United States
June 2, 2006 through June 3, 2006

Disclaimer

Use of Commercial I&C in the Next Generation of Nuclear Power (and Other Thoughts)

Presented to:
Technology Roadmap Workshop on Instrumentation, Control, and Human Machine Interface to Support DOE Advanced Nuclear Power Plant Programs

Reno, Nevada
June 2, 2006

Gary Johnson
Lawrence Livermore National Laboratory

We should position ourselves to take better advantage of commercial equipment

- New technologies will always emerge first in commercial applications
  - Simply; there is a larger market
  - Developing only to nuclear needs risks marketing dead-end
  - Exception, nuclear specific functions and equipment
- Many needed technologies already exist
  - Network field devices
  - Wireless field devices
  - Battery powered field devices
  - Intelligent field devices
  - Multivariable transmitters
  - Visualization
  - Industrial network protocols
  - Mini signal conditioners
  - Modern displays
  - Modern flow, level, and temperature sensors
    - Not so much new ideas, but old new ideas have proven themselves
  - Alarm management
- In the last 15 years industry has introduced formal requirements for the integrity of safety functions, systems, and equipment
  - Examples: IEC 61508, ISA SP84, UL 1998
  - AIChE has driven much of this work in response to chemical process accidents and OSHA requirements

The industry is taking certification for safety application seriously

- Rosemount PT, TT
- Green Hills RTOS
- Phoenix Contract relays
- Yokogawa ProSafe PLC
- ABB Metcon PT
- Triconix Trident PLC
- Emerison Delta V logic solver
- Emerison Fieldvue valve controller
- Maxcon air operated valves
- ADS Tech single board computer
- Wind River RTOS
- Honneywell SafetyManager PLC
- CanOpen microcontroller
- Allen-Bradley GuardPLC
- Schmersal limit switches
- Siemens AS-I limit switches, position sensors, light curtains, logic
- Samson 3730 positioner
- Ominfles annunciators
- Yokogawa EJX pressure transmitters

We need ways to take advantage of these certifications rather than starting from zero

There will be gaps

	61508	System	Plant	Gap
Performance requirements	X	X		
Design for reliability	X	X		
Single failure criterion	X	X		
Redundancy	X	X		
Diversity	X	X		
Reliability assessment	X	X		
Software reliability	X			
Independence	X	X		
Failure modes	X	X		
Control of access to equipment		x		
Set points		X		
Human–machine interface		X		
Equipment qualification	X			*
Quality	X		x	*
EMI compatibility	X	x		*
Testing and testability	X			
Test programme			x	
Fault detection	X			
Demonstration of sys temp erformance	X	x		
Removal from service	X	x		
Maintainability	X			
Documentation	x	x		
Identification of items important to safety		x		

This table is illustrative only. A thorough comparison is needed and other industry standards beyond IEC 61508 should be considered.
*In these cases IEC 61508 addresses the topic, but the detailed environments are different

Bridging these gaps will bring commercial technology to our market more quickly

- Understand what are the gaps
- Encourage vendors toward certification
  - Show them an edge in the nuclear market
  - Show them more credibility in the industrial market
- Make certification easier
  - Foster and certify certifiers (similar to TuV in Germany)
- Help vendors bridge the gaps
  - Foster improvement to their own processes and methods where doing so will also give them a commercial advantage
  - Provide a path forward for bridging nuclear-specific gaps
    - Feasibility assessment
    - Implementation support

A couple of dissociated thoughts

- **Does presence of diverse actuation allow for simpler protection system architectures or relaxed requirements in some areas?**
- **Can diversity be built into the design rather that being hung on afterwards**
  - **System 80+ was a case where intelligent (fortuitous?) design of protection and control eliminated the need for diverse protection**
  - **Extend consideration of diversity to mechanical systems**
    - **e.g., safety valves and power operated relief valves are diverse means for protecting against overpressure**

      Only the later involve electronics
- **What the heck is diversity anyway?**
  - **What types of CCF actually happen?**
  - **Are there design strategies that would implement diversity in a more organic way, reducing the need for diverse equipment or software?**
    - **e.g., running PLC statement lists in different order in redundant channels**
- **What software design strategies simplify qualification?**
- **To what degree can experience be used to accept functions where the application is not variable or where experience is gained over a broad range of signal trajectories**
  - **E.g., communications networks, equipment, and protocols**

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.